OPIC

November 8, 2018

Ms. Emma Best
MuckRock News
411A Highland Avenue
Dept. MR 49294
Somerville, Massachusetts 02144

RE: Response for OPIC FOIA Request 2019-00004, NARA NGC18-367

Dear Ms. Best,

You filed Freedom of Information Act ("FOIA") requests with the National Archives and Records Administration (NARA) for each agency's SF-716 forms. NARA referred the forms submitted by the Overseas Private Investment Corporation (OPIC) to our agency for direct response to you. OPIC received this referral on November 2, 2018 and assigned it **FOIA Number 2019-00003**. Please reference this number in all correspondence.

OPIC is releasing the records referred by NARA in part. Partial withholdings have been made under Exemptions b(5) and b(6). The FOIA contains nine exemptions which allow an agency to withhold information from release.

Exemption b(5) protects "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency." 5 U.S.C. § 552(b)(5) (2012). These forms were submitted between OPIC and NARA, two federal agencies and are therefore inter-agency records. OPIC has used Exemption b(5) to withhold portions of the records which contain sensitive information about OPIC's security program.

Exemption b(6) of the FOIA protects information about individuals in "personnel and medical files and similar files" when the disclosure of such information "would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6). The exemption was meant to be interpreted broadly and is not tied to the label of the file containing the information. United States Department of State v. Washington Post Co., 456 U.S. 595 (1982). Exemption b(6) is therefore applied when the private interest in keeping personal information is greater than the public interest in disclosure. Dep't of the Air Force v. Rose, 425 U.S. 352, 372 (1976). The only public interest relevant in a b(6) inquiry is the public interest in knowing what the government is up to. Dep't of Defense v. Fed. Labor Rel'n Auth., 510 U.S. 487, 497 (1994). OPIC has used Exemption b(6) to withhold the direct contact information of its staff. This

Overseas Private Investment Corporation
1100 New York Avenue, NW
Washington, D.C. 20527
202.336.8400 | www.opic.gov

information is tied to an individual and shows no government action. OPIC has also used Exemption b(6) to withhold the identity of the OPIC staff who were the contacts for the forms Revealing their identity would reveal their security clearances, which is personal information that does not reveal government action. The identity of the senior official in charge of OPIC's security has been left intact as this is the official who bears the responsibility of ensuring the agency's compliance.

This is a final agency response. You may contact me or the FOIA Public Liaison for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about FOIA dispute resolution services they offer. The contact information for OGIS is as follows:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road-OGIS
College Park, MD 20740-6001
Email: ogis@nara.gov
Phone: 202-741-5770 | Toll Free: 877-684-6448 | Fax: 202-741-5769

If you are not satisfied with OPIC's response to this request, you may administratively appeal by addressing a written appeal to the following:

Deputy General Counsel
Overseas Private Investment Corporation
1100 New York Ave., N.W.—12th Floor
Washington, D.C. 20527

Your appeal must be postmarked or electronically transmitted **within 90 days** of the date of this response to your request. Both the envelope and the letter should be marked "FREEDOM OF INFORMATION ACT APPEAL." The appeal should clearly identify the agency determination that is being appealed and include the request number. If you are not satisfied with the results of any such appeal, judicial review is available to you in the United States District Court for the judicial districts in which you reside or have your principal place of business, or in the District of Columbia.

Sincerely,

Nichole Skoyles
Administrative Counsel
Overseas Private Investment Corporation
1100 New York Avenue, N.W.
Washington, D.C. 20527
202.408.6297 | Nichole.Skoyles@opic.gov

1100 New York Avenue, N.W.
Washington, D.C. 20527-0001
(202) 336-8400
FAX (202) 408-9859

March 21, 2003

Laura L.S. Kimberly
Associate Director for Policy
Information Security Oversight Office
National Archives and Records Administration
700 Pennsylvania Avenue, NW
Washington, DC 20408

Subject: Report on Cost Estimates for Security Classification Activities

Dear Ms Kimberly:

Reference your letter dated February 7, 2003, subject as above.

Attached is a report addressing cost estimates for security classification activities for the Overseas Private Investment Corporation for Fiscal Years 2002, 2003, and 2004.

If you need additional information, please contact the undersigned at (b) (6)

Regards,

(b) (6)

(b) (6) Contract and Administrative Services

Attachment as Stated

2004 Security Costs Estimates Display

Name of Department/Agency: OVERSEAS PRIVATE INVESTMENT CORPORATION

Reporting Categories	FY 2002 (Est. in $000s)	FY 2003 (Est. in $000s)	FY 2004 (Est. in $000s)
1. Personnel Security	76	62	61
2. Physical Security	7	18	5
3. Information Security (Sum of *a,b* & c below)	6	5	5
a. Classification Management	6	5	5
b. Declassification	0	0	0
c. Information Technology (Electronic Security)	0	0	0
4. Professional Education, Training and Awareness	0	1	1
5. Security Management, Oversight and Planning	12	14	14
6. Unique Items	0	0	0
Totals: Fiscal Year Estimates	101	100	86
Totals: Full-Time Equivalents (FTE)	.4	.5	.5

NARRATIVE:

SEE ATTACHED COMMENTS

3/21/03

2004 Security Cost Estimates

1. Personnel Security
   FY 02 $76K
   - estimate is based on $63K actual cost incurred to obtain security clearances for FTEs
   - 10% of $126K (GS15 salary plus 24% fringe benefits) for administration cost

   FY 03 $62K
   - estimate is based on $40K budgeted to obtain security clearances for FTEs
   - 10% of $130K (GS15 salary plus 24% fringe benefits) for administration cost
   - Background investigations for 40 contractor staff personnel @$95 per investigation
   - 10% of $45K (GS7 salary plus 24% fringe benefits) for administration cost of contractor background investigations

   FY 04 $61K
   - estimate is based on $40K budgeted to obtain security clearances for FTEs
   - 10% of $136K (GS15 salary plus 24% fringe benefits) for administration cost
   - background investigations for 10 contractor staff personnel @$95 per investigation
   - 10% of $56K (GS9 salary plus 24% fringe benefits) for administration cost of contractor background investigations

2. Physical Security
   FY02 $7K
   - 10% of $66K (GS11 salary plus 24% fringe benefits) for administration

   FY03 $18K
   - estimate is based on 10% of $45K (GS7 salary plus 24% fringe benefits)
   - 10% of $131K (GS14 salary plus 24% fringe benefits)

3/21/03

FY04 $5K

- estimate is based on 10% of $45K (GS7 salary plus 24% fringe benefits)

3. Information Security

a. Classification Management- Estimate for each fiscal year is based on 10% of a FTE.

FY02	FY03	FY04
$6K	$5K	$5K

b. Declassification- No declassification activity

c. Information Technology - 0

4. Professional Education, Training and Awareness

FY02	FY03	FY04
0	$1K	$1K

5. Security Management, Oversight and Planning - Estimate is based on 10% of GS14 salary for each year.

FY02	FY03	FY04
$12K	$14K	$14K

OPIC Overseas Private Investment Corporation

1100 New York Avenue, N.W.
Washington, D.C. 20527-0001
(202) 336-8400
FAX (202) 408-9859

March 19, 2004

Ms. Laura L.S. Kimberly
Associate Director for Policy
Information Security Oversight Office
National Archives and Records Administration
700 Pennsylvania Avenue, N.W.
Washington, DC 20408

Subject: Report on Cost Estimates for Security Classification Activities

Dear Ms. Kimberly:

Attached is a report addressing cost estimates for security classification activities for the Overseas Private Investment Corporation for Fiscal Years 2003, 2004, and 2005.

If you need additional information, please contact me at (b) (6)

Sincerely,

(b) (6)

(b) (6) Security & Administrative Services

Attachment as Stated

2005 Security Costs Estimates Display

Name of Department/Agency: Overseas Private Investment Corporation

Reporting Categories	FY 2003 (Est. in $000s)	FY 2004 (Est. in $000s)	FY 2005 (Est. in $000s)
1. Personnel Security	62	63	65
2. Physical Security	20	98	101
3. Information Security (Sum of *a, b,* c & d below)	5	7	73
a. Classification Management	5	5	8
b. Declassification	0	0	0
c. Information Systems Security	0	2	65
d. Miscellaneous (OPSEC & TSCM)	0	0	0
4. Professional Education, Training and Awareness	1	5	5
5. Security Management, Oversight and Planning	14	14	14
6. Unique Items	0	0	0
Totals: Fiscal Year Estimates	102	187	258
Totals: Full-Time Equivalents (FTEs)	.5	1	1.5

NARRATIVE: See attached.

Security Cost
Basis of Estimates

1. Personnel Security

FY 03 $62K

- estimate is based on $40K budgeted to obtain security clearances for OPIC FTEs
- personnel salary, 10% of $130K (GS15 salary plus 24% fringe benefits) for administration cost
- personnel salary, 10% of $45K (GS7 salary plus 24% fringe benefits) for administration cost of contractor background investigations
- background investigations for 40 contractor staff personnel @$95 per investigation

FY 04 $63K

- estimate is based on $40K budgeted to obtain security clearances for FTEs
- personnel salary, 10% of $141K (GS15/5 ($114K) salary plus 24% fringe benefits) for administration cost
- personnel salary, 10% of $58K (GS9/5 ($47K) salary plus 24% fringe benefits) for administration cost of contractor background investigations
- background investigations for 30 contractor staff personnel @$120 per investigation

FY 05 $65K

- estimate is based on $40K budgeted to obtain security clearances for OPIC FTEs
- personnel salary, 10% of $141K (GS15/5 ($114K) salary plus 24% fringe benefits) for administration cost
- personnel salary, 10% of $76K (GS12/1 ($61K) salary plus 24% fringe benefits) for administration cost of contractor background investigations
- background investigations for 30 contractor staff personnel @$120 per investigation

2. **Physical Security**

FY03 $20K

- personnel salary, estimate based on 10% of $45K (GS7 ($36K) salary plus 24% fringe benefits)
- personnel salary, 10% of $141K (GS15/5 ($114K) salary plus 24% fringe benefits)

FY04 $98K

- personnel salary, estimate is based on 10% of $58K (GS9/5 ($47K) salary plus 24% fringe benefits)
- upgrade security & alarm systems, $25K
- implement new badging system, $15K

FY05 $101K

- personnel salary, estimate is based on 10% of $76K (GS12/1 ($61K) salary plus 24% fringe benefits)
- Install CCTV, $25K

3. **Information Security**

a. Classification Management- Personnel salary estimate for each fiscal year is based on 10% of a FTE, (FY05 cost is based on GS 12/1 ($61K) salary plus 24% fringe benefits)

FY03	**FY04**	**FY05**
$5K	$5K	$8K

b. Declassification- No declassification activity

c. Information Technology - Install CableExpress ($60K), and install 2 analog lines in Rm 11163 @ $400.mo.

FY03	**FY04**	**FY05**
0	$2400	$64,800

d. Miscellaneous (OPSEC & TSCM)- No activity

4. **Professional Education, Training and Awareness -**
Security Specialist Course-DSS, 3 weeks
COMSEC training at NSA- 1 week
Physical Security Course at DSS (2 people)-2 weeks

FY03	FY04	FY05
$1K	$5K	$5K

5. **Security Management, Oversight and Planning -** Personnel salary, estimate is based on 10% of $141K (GS15/5 ($114K) salary plus 24% fringe benefits).

FY03	FY04	FY05
$14K	$14K	$14K

FY2004

FY 2006 Security Cost Estimates Display

Name of Department/Agency: Overseas Private Investment Corporation

(Please use actual dollar figures instead of thousands.)

Reporting Categories	FY 2004	FY 2005	FY 2006
1. Personnel Security	$63,000.00	$78,000.00	$82,000.00
2. Physical Security	$98,000.00	$201,000.00	$246,000.00
3. Information Security			
(a.) Classification Management	$5,000.00	$9,600.00	$9,900.00
(b.) Declassification	$10,000.00	$20,000.00	$15,000.00
(c.) Information Systems Security for Classified Information	0	$2,400.00	$75,000.00
(d.) Miscellaneous (OPSEC & TSCM)	0	0	0
(e.) Information Security Subtotal (Sum of 3.a., 3.b., 3.c., & 3.d.)	$15,000.00	$32,000.00	$99,900.00
4. Professional Education, Training and Awareness	$5,000.00	$6,000.00	$8,000.00
5. Security Management, Oversight and Planning	$14,000.00	$9,600.00	$10,000.00
6. Unique Items	0	0	0
Totals: Fiscal Year Estimates (Sum of 1, 2, 3(e.), 4, 5, & 6)	$195,000.00	$326,600.00	$445,900.00

NARRATIVE: See attached

OK

OPIC Overseas Private Investment Corporation

1100 New York Avenue, N.W.
Washington, D.C. 20527-0001
(202) 336-8400
FAX (202) 408-9859

March 31, 2006

Mr. J. William Leonard
Director
Information Security Oversight Office
National Archives and Records Administration
700 Pennsylvania Avenue, N.W.
Washington, DC 20408

Subject: Report on Cost Estimates for Security Classification Activities

Dear Mr. Leonard:

Attached is our report on cost estimates for security classification activities for the Overseas Private Investment Corporation.

If you need additional information, please contact me at (b) (6)

Sincerely,

(b) (6)

(b) (6) Security & Administrative Services

Attachment as Stated

Security Costs Estimates Display

Name of Department/Agency: Overseas Private Investment Corporation

(Please use actual dollar figures instead of thousands)

Reporting Categories	FY 2005	FY 2006	FY 2007
1. Personnel Security	$78,000.00	$82,000.00	$93,100.00
2. Physical Security	$201,000.00	$246,000.00	$107,800.00
3. Information Security			
(a.) Classification Management	$9,600.00	$9,900.00	$8,000.00
(b.) Declassification	$20,000.00	$15,000.00	$10,000.00
(c.) Information Systems Security for Classified Information	$2,400.00	$75,000.00	$75,000.00
(d.) Miscellaneous (OPSEC & TSCM)	0	0	0
(e.) Information Security Sub-Total *(Sum of 3.a., 3.b., 3.c., & 3.d.)*	$32,000.00	$99,900.00	$93,000.00
4. Professional Education, Training and Awareness	$6,000.00	$8,000.00	$8,000.00
5. Security Management, Oversight and Planning	$9,600.00	$10,000.00	$8,000.00
6. Unique Items	0	0	0
Totals: Fiscal Year Estimates (Sum of 1, 2, 3(e.), 4, 5, & 6.)	$326,600.00	$445,900.00	$309,900.00

NARRATIVE: see attached

Security Cost
Basis of Estimates

1. Personnel Security

FY 05 $78K

- estimate is based on $45K budgeted to obtain security clearances for OPIC FTEs
- personnel salary, 10% of $146K (GS15/5 ($118K) salary plus 24% fringe benefits) for administration cost
- personnel salary, 10% of $96K (GS13/2 ($77K) salary plus 24% fringe benefits) for administration cost of contractor background investigations
- background investigations for 30 contractor staff personnel @$130 per investigation

FY 06 $82K

- estimate is based on $48K budgeted to obtain security clearances for OPIC FTEs
- personnel salary, 10% of $150K (GS15/5 ($120K) salary plus 24% fringe benefits) for administration cost
- personnel salary, 10% of $99K (GS13/2 ($79K) salary plus 24% fringe benefits) for administration cost of contractor background investigations
- background investigations for 30 contractor staff personnel @$135 per investigation

NOTE: The $82K that we estimated in last year's report will be lower due to staff turnover. The GS13 left the end of August 2005 and was replaced with a GS12 in January FY06.

FY 07 $93K

- estimate is based on $65K budgeted to obtain security clearances for OPIC FTEs
- personnel salary, 10% of $159K (GS15/7 ($129K) salary plus 24% fringe benefits) for administration cost
- personnel salary, 10% of $80K (GS12/1 ($65K) salary plus 24% fringe benefits) for administration cost of contractor background investigations

- background investigations for 30 contractor staff personnel @$140 per investigation

2. **Physical Security**

FY05 $201K

- personnel salary, estimate is based on 10% of $96K (GS13/2 ($77K) salary plus 24% fringe benefits)
- Upgrade of security and alarm systems, $25K
- Implement new HSPD/12 badging system, $30K
- Visitor control for personnel and activities, based on 10% of guard costs, $50K

FY06 $246K

- personnel salary, estimate is based on 10% of $99K (GS13/2 ($79K) salary plus 24% fringe benefits)
- Install CCTV, $30K
- HSPD/12 initiative – upgrade of access control equipment, $65K
- Visitor control for personnel and activities, based on 10% of guard costs, $52K

NOTE: The $246K that we estimated in last year's report will be lower due to changing governmental priorities and lack of funding. We did not have funds allotted for bullets 2-3 in FY2006. We also had staff turnover - the GS13 left the end of August 2005 and was replaced with a GS12 in January FY06.

FY07 $107K

- personnel salary, 10% of $80K (GS12/1 ($65K) salary plus 24% fringe benefits) for administration cost of contractor background investigations
- Install CCTV, $30K
- HSPD/12 initiative – upgrade of access control equipment, $65K
- Visitor control for personnel and activities, based on 10% of guard costs, $48K

3. **Information Security**

3.a.

a. Classification Management- Personnel salary estimate for each fiscal year is based on 10% of a FTE, (FY05 cost is based on GS 13/2 ($77K) salary plus 24% fringe benefits)
NOTE: The FY06 cost that we estimated in last year's report will be lower due to staff turnover. The GS13 left the end of August 2005 and was replaced with a GS12 in January FY06.

FY05	FY06	FY07
$9600K	$9900K	8000K

3.b.

b. Declassification- Personnel salary estimate for each fiscal year based on number of estimated hours multiplied by hourly rate of FTE/contractors
NOTE: We expect the declassification costs to decrease in 2007.

FY05	FY06	FY07
$20K	$15K	$10K

3.c.

c. Information Technology - Install CableExpress ($70K), and install 2 analog lines in Rm 11163 @ $400.mo.
NOTE: The FY2006 cost that we estimated in last year's report was not funded. We also had staff turnover that impacted this initiative.

FY05	FY06	FY07
$2400	$75K	$75K

3.d.

d. Miscellaneous (OPSEC & TSCM)- No activity

FY05	FY06	FY07
0	0	0

4. **Professional Education, Training and Awareness** -
Security Specialist Course-DSS, 3 weeks
Physical Security Course at DSS (2 people)-2 weeks
Miscellaneous security conferences and training courses

FY05	FY06	FY07
$6K	$8K	$8K

5. **Security Management, Oversight and Planning** - Personnel salary, estimate is based on 10% of $96K (GS13/2 ($77K) salary plus 24% fringe benefits).
NOTE: The FY06 cost that we estimated in last year's report will be lower due to staff turnover. The GS13 left the end of August 2005 and was replaced with a GS12 in January FY06.

FY05	FY06	FY07
$9600K	$10K	$8K

OPIC Overseas Private Investment Corporation

1100 New York Avenue, N.W.
Washington, D.C. 20527-0001
(202) 336-8400
FAX (202) 408-9859

March 7, 2008

Mr. William J. Bosanko
Acting Director
Information Security Oversight Office
National Archives Building
Room 500
700 Pennsylvania Avenue, N.W.
Washington, D.C. 20408-0001

RE: Report on Cost Estimates for Security Classification Activities

Dear Mr. Bosanko:

Attached is our FY2007 report on cost estimates for security classification activities for the Overseas Private Investment Corporation.

Please do not hesitate to contact me at (b) (6) if you need additional information.

Sincerely,

(b) (6)

(b) (6)
Security & Administrative Services
Overseas Private Investment Corporation
1100 New York Ave. N.W.
Washington, D.C. 20527

Attachment as Stated

Security Costs Estimates Report

Name of Department/Agency: Overseas Private Investment Corporation

(Please use actual dollar figures instead of thousands)

Reporting Categories	FY 2007
1. Personnel Security	$77,902.55
2. Physical Security	$16,637.70
3. Information Security	
(a.) Classification Management	$1,234.20
(b.) Declassification	$25,386.70
(c.) Information Systems Security for Classified Information	$0
(d.) Miscellaneous (OPSEC & TSCM)	$0
(e.) Information Security Sub-Total *(Sum of 3.a., 3.b., 3.c., & 3.d.)*	$26,620.90
4. Professional Education, Training and Awareness	$0
5. Security Management, Oversight and Planning	$21,183.20
6. Unique Items	$0
Totals: Fiscal Year Estimates (Sum of 1, 2, 3(e.), 4, 5, & 6.)	$142,344.35

NARRATIVE: See attached

OPIC 2007 Report on Cost Estimates for Security Classification Activities
Basis of Estimates

1. **Personnel Security - FY 07 $77,902.55**

   - estimate is based on $52,000.00 to obtain security clearances for OPIC FTEs
   - personnel salary, 10% of $132,435.00 (GS15/7)
   - personnel salary, 15% of $79,397.00 (GS13/1)
   - $750.00 for background investigations for contractor staff personnel

2. **Physical Security - FY07 $16,637.70**

   - personnel salary, estimate is based on 10% of $79,397.00 (GS13/1)
   - Visitor control for personnel and activities, based on 5% of guard costs ($43,490.00)

3. **Information Security - FY07 - $34,560.60**

a. Classification Management -
   - $7,939.70 - Personnel salary estimate is based on 10% of $79,397.00 (GS 132/1)
   - $1,234.20 - Cost of OPIC files housed at WNRC that contain classified material

b. Declassification- $25,386.70
   Estimated cost includes WNRC services, State Dept. declassification office services, and OPIC personnel salary.

c. Information Technology -
   $0

d. Miscellaneous (OPSEC & TSCM)
   $0

4. **Professional Education, Training and Awareness - FY07 - $0**

   Attended miscellaneous government sponsored security conferences and training

5. **Security Management, Oversight and Planning - FY07 - $21,183.20**

   Personnel salary, estimate is based on 10% of $79,397.00 (GS 11/1) and personnel salary, 10% of $132,435.00 (GS15/7)

6. **Unique items: FY07 - $0**

Security Costs Estimates Display

Name of Department/Agency: Overseas Private Investment Corporation

(Please use actual dollar figures instead of thousands)

Reporting Categories	FY 2008
1. Personnel Security	$86,637.75 86,638
2. Physical Security	$28,710.35 28,710
3. Information Security	
(a.) Classification Management	$19,287.50 19288
(b.) Declassification	0
(c.) Information Systems Security for Classified Information	0
(d.) Miscellaneous (OPSEC & TSCM)	0
(e.) Information Security Sub-Total (Sum of 3.a., 3.b., 3.c., & 3.d.)	$19,287.50 19288
4. Professional Education, Training and Awareness	0
5. Security Management, Oversight and Planning	$22,795.40 22,795
6. Unique Items	0
Totals: Fiscal Year Estimates (Sum of 1, 2, 3(e.), 4, 5, & 6.)	$157,431.00 ✓ 157,431 ✓

NARRATIVE:

OPIC Overseas Private Investment Corporation

1100 New York Avenue, N.W.
Washington, D.C. 20527-0001
(202) 336-8400
FAX (202) 408-9859

February 26, 2010

Mr. William J. Bosanko
Director
Information Security Oversight Office
National Archives Building
700 Pennsylvania Avenue, N.W.
Washington, D.C. 20408-0001

RE: Report on Cost Estimates for Security Classification Activities

Dear Mr. Bosanko:

Attached is our FY2009 report on cost estimates for security classification activities for the Overseas Private Investment Corporation.

Please do not hesitate to contact me at (b) (6) if you need additional information.

Sincerely,

(b) (6)

(b) (6)
Security & Administrative Services
Overseas Private Investment Corporation
1100 New York Ave. N.W.
Washington, D.C. 20527

Attachment as Stated

Security Costs Estimates Display

Name of Department/Agency: Overseas Private Investment Corporation

Point of contact (Name/phone number): (b) (6)

(Please use actual dollar figures instead of thousands)

Reporting Categories	FY 2009
1. Personnel Security	$109,047.10
2. Physical Security	$33,137.30
3. Information Security	
(a.) Classification Management	$ 17,303.05
(b.) Declassification	0
(c.) Information Systems Security for Classified Information	0
(d.) Miscellaneous (OPSEC & TSCM)	0
4. Professional Education, Training and Awareness	0
5. Security Management, Oversight and Planning	$24,174.80
6. Unique Items	0
Totals: Fiscal Year Estimates (Sum of 1, 2, 3(a),3(b),3(c),3(d) 4, 5, & 6.)	**$ 183,662.25**

NARRATIVE: see attached

OPIC 2009 Report on Cost Estimates for Security Classification Activities
Basis of Estimates

1. **Personnel Security - FY09 $109,047.10**

   - estimate is based on $75,00.00 to obtain security clearances for OPIC FTEs
   - personnel salary, 10% of $149,025.00 (GS15/8)
   - personnel salary, 20% of $92,723.00 (GS13/2)
   - $600.00 for background investigations for contractor staff personnel

2. **Physical Security - FY09 $33,137.30**

   - personnel salary, estimate is based on 10% of $92,723.00 (GS13/3)
   - Visitor control for personnel and activities, based on 5% of guard costs ($58,500.00)
   - Access control system maintenance & monitoring - $20,940.00

3. **Information Security - FY09 - $17,303.05**

a. Classification Management -
   - $9,851.80 - Personnel salary estimate is based on 10% of $98,518.00 (GS 13/5)
   - $7,451.25 - personnel salary, 5% of $149,025.00 (GS15/8)

b. Declassification-
   $0

c. Information Technology -
   $0

d. Miscellaneous (OPSEC & TSCM)
   $0

4. **Professional Education, Training and Awareness - FY09 - $0**

   Attended miscellaneous government sponsored security conferences and training

5. **Security Management, Oversight and Planning - FY09 - $24,174.80**

   Personnel salary, estimate is based on 10% of $92,723.00 (GS 13/3) and personnel salary, 10% of $149,025.00 (GS15/8)

6. **Unique items: FY09 - $0**

OPIC Overseas Private Investment Corporation

1100 New York Avenue, N.W.
Washington, D.C. 20527-0001
(202) 336-8400
FAX (202) 408-9859

February 25, 2011

Mr. William J. Bosanko
Director
Information Security Oversight Office
National Archives Building
700 Pennsylvania Avenue, N.W.
Washington, D.C. 20408-0001

RE: Report on Security Cost Estimates

Dear Mr. Bosanko:

Attached is our FY2010 report on security cost estimates for the Overseas Private Investment Corporation.

Please do not hesitate to contact me at (b) (6) if you need additional information.

Sincerely,

(b) (6)

(b) (6)
Security & Administrative Services
Overseas Private Investment Corporation
1100 New York Ave. N.W.
Washington, D.C. 20527

Attachment as Stated

Security Costs Estimates

Department/Agency: Overseas Private Investment Corporation **Fiscal Year:** 2010

Point of Contact: (Name and phone number) (b) (6) Security & Administrative Services

Reporting Categories

(Please use actual dollar figures instead of thousands)

1. Personnel Security $63,697.05

(Include clearance program, initial investigations, national agency checks when used for basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification related activities)

2. Physical Security $488,892.54

(Include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification related activities)

3. Information Security

(only report costs associated with classification related activities)

(a) Classification Management $17,568.60

(Include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)

(b) Declassification $0.00

(include resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive order or statute)

(c) Information Systems Security for Classified Information $0.00

(Include resources used to protect information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)

(d) Miscellaneous (OPSEC and TSCM) $0.00

(Include personnel and operating expenses associated with these programs)

4. Professional Education, Training, and Awareness $2,300.00

(Include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification related activities)

5. Security Management, Oversight, and Planning $48,672.60

(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))

6. Unique Items $0.00

(Include department/agency-specific activities not reported in any of the categories listed above but are nonetheless significant and need to be included)

Total (sum of 1, 2, 3(a), 3(b), 3(c), 3(d), 4, 5, and 6) $621,130.79

Narrative: *provide a brief explanation of any significance difference between last year's and this year's cost estimates. Explain items entered into Block 6. Unique Items.*

In 2010, OPIC signed an inter-agency agreement with GSA to receive PIV card issuance and support through a GSA managed service offering as part of the USAccess Program. Using a USAccess contract registrar, we issued HSPD-12 PIV cards to agency employees. We also worked with a consultant and integrator to replace our Physical Access Control System.

OPIC 2010 Security Cost Estimates

1. Personnel Security – FY 2010 - **$63,697.05**

   - Estimate is based on $20,491.85 to obtain security clearances for OPIC FTEs
   - Personnel salary – 10% of $155,500 (GS15/9)
   - Personnel salary – 20% of $97,936 (GS13/4)
   - Personnel salary – 3% of $105,211 (GS14/1)
   - Personnel Salary – 3% of $115,731 (GS14/4)
   - Personnel Salary – 2% of $54,534 (GS8/6)
   - $400.00 for background investigations for contractor staff personnel

2. Physical Security – FY2010 - **$488,892.54**

   - Personnel salary – 25% of $155,500 (GS15/9)
   - Personnel salary – 10% of $97,936 (GS13/4)
   - Visitor control for personnel and activities, based on 5% of guard costs (57793.28)
   - Access control system consultant and system replacement, intrusion detection - $411,753.28
   - HSPD-12 badges USAccess system (contract registrar and badges) - $25,577.00

3. Information Security – FY2010 - **$17,568.60**

   - Classification management
     Personnel salary estimate is based on 10% of $97,936 (GS13/4)
     Personnel salary estimate based on 5% of $155,500 (GS15/9)
   - Declassification - $0
   - Information Systems Security for Classified Information - $0
   - Miscellaneous - $0

4. Professional Education, Training, and awareness – FY2010 - **$2,300.00**

   - Security Professionals Seminar - $300.00
   - C-Cure system training - $2,000.00

5. Security Management, Oversight, and Planning - **$48,672.60**
   - Personnel salary estimate based on 25% of $155,500 (GS15/9)
   - Personnel salary estimate based on 10% of $97,936 (GS13/4)

6. Unique items - $0

OPIC Overseas Private Investment Corporation

1100 New York Avenue, N.W.
Washington, D.C. 20527-0001
(202) 336-8400
FAX (202) 408-9859

February 29, 2012

Mr. John P. Fitzpatrick
Director
Information Security Oversight Office
National Archives Building
700 Pennsylvania Avenue, N.W.
Washington, D.C. 20408-0001

RE: Report on Security Cost Estimates

Dear Mr. Fitzpatrick:

Attached is our FY2011 report on security cost estimates for the Overseas Private Investment Corporation.

Please do not hesitate to contact me at (b) (6) if you need additional information.

Sincerely,

(b) (6)

(b) (6)
Security & Administrative Services
Overseas Private Investment Corporation
1100 New York Ave. N.W.
Washington, D.C. 20527

Attachment as Stated

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: Overseas Private Investment Corporation	**Fiscal Year:** 2011

Point of Contact:
(Name and phone number) (b) (6) Security & Administrative Services (b) (6)

Reporting Categories

Please use actual dollar figures.

1. Personnel Security *(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)*	$70,289.80
2. Physical Security *(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)*	$64,271.47
3. Classification Management *(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)*	$17,865.40
4. Declassification *(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)*	$0.00
5. Protection and Maintenance for Classified Information Systems *(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)*	$0.00
6. Operations Security and Technical Surveillance Countermeasures *(include personnel and operating expenses associated with OPSEC and TSCM)*	$0.00
7. Professional Education, Training, and Awareness *(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)*	$150.00
8. Security Management, Oversight, and Planning *(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))*	$48,965.40
9. Unique Items *(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)*	$0.00
TOTAL *(sum of items 1-9)*	$201,542.07

Narrative: *Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.*

Physical access control system replacement was completed in FY2010. FY2011 costs reflect maintenance and monitoring of PACS.

OPIC 2011 Security Cost Estimates

1. Personnel Security – FY 2011 - **$70,289.80**

   - Estimate is based on $25,000.00 to obtain security clearances for OPIC FTEs
   - Personnel salary – 10% of $155,500 (GS15/10) - $15,500.00
   - Personnel salary – 20% of $100,904 (GS13/5) – 20,180.80
   - Personnel salary – 3% of $136,771 (GS14/10) - $4,103.00
   - Personnel Salary – 3% of $127,883 (GS15/2) - $3,836.00
   - Personnel Salary – 2% of $58,511 (GS9/5) – 1170.00
   - $500.00 for background investigations for contractor staff personnel

2. Physical Security – FY2011 - **$ 64,271.47**

   - Personnel salary – 25% of $155,500 (GS15/10) - $38,875.00
   - Personnel salary – 10% of $100,901 (GS13/5) - $10,090.40
   - Visitor control for personnel and activities, based on 5% of guard costs (57,841.46) – 2,892.07
   - Access control system maintenance & monitoring - $ 4,020.00
   - HSPD-12 badges USAccess system (contract registrar and badges) - $ 8,394.00

3. Information Security – FY2011 - **$ 17,865.40**

   - Classification management
     Personnel salary estimate is based on 10% of $100,904 (GS13/5) – 10,090.40
     Personnel salary estimate based on 5% of $155,500 (GS15/10) - $7,775.00
   - Declassification - $0
   - Information Systems Security for Classified Information - $0
   - Miscellaneous - $0

4. Professional Education, Training, and awareness – FY2011 - **$ 150.00**

   - Security Professionals Seminar - $ 150.00
   -

5. Security Management, Oversight, and Planning - **$ 48,965.40**
   - Personnel salary estimate based on 25% of $155,500 (GS15/10) - $38,875.00
   - Personnel salary estimate based on 10% of $100,904 (GS13/5) -$10,090.40

6. Unique items - $0

OPIC Overseas Private Investment Corporation

1100 New York Avenue, N.W.
Washington, D.C. 20527-0001
(202) 336-8400
FAX (202) 408-9859

February 28, 2013

Mr. John P. Fitzpatrick
Director
Information Security Oversight Office
National Archives Building
700 Pennsylvania Avenue, N.W.
Washington, D.C. 20408-0001

RE: Report on Security Cost Estimates

Dear Mr. Fitzpatrick:

Attached is our FY2012 report on security cost estimates for the Overseas Private Investment Corporation.

Please do not hesitate to contact me at (b) (6) if you need additional information.

Sincerely,

(b) (6)

(b) (6)
Security & Administrative Services
Overseas Private Investment Corporation
1100 New York Ave. N.W.
Washington, D.C. 20527

Attachment as Stated

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: Overseas Private Investment Corporation	**Fiscal Year:** 2012

Point of Contact:
(Name and phone number) (b)(6) [redacted]

Reporting Categories

Please use actual dollar figures.

1. Personnel Security *(Include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)*	$154,763.22
2. Physical Security *(Include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)*	$46,483.25
3. Classification Management *(Include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)*	$20,590.25
4. Declassification *(Include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)*	$1,038.70
5. Protection and Maintenance for Classified Information Systems *(Include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)*	$979.36
6. Operations Security and Technical Surveillance Countermeasures *(Include personnel and operating expenses associated with OPSEC and TSCM)*	$0.00
7. Professional Education, Training, and Awareness *(Include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)*	$2,500.00
8. Security Management, Oversight, and Planning *(Include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))*	$60,749.70
9. Unique Items *(Include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)*	$0.00
TOTAL *(sum of items 1-9)*	$287,104.48

Narrative: *Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.*

OPIC 2012 Security Cost Estimates

1. Personnel Security – FY 2012 - **$154,763.22**

   - Estimate is based on $122,384,53 to obtain security clearances for OPIC FTEs
   - Personnel salary – 5% of $155,500 (GS15/10) - $7,775.00
   - Personnel salary – 20% of $97,936.00 (GS13/4) – $19,587.20
   - Personnel Salary – 3% of $127,883 (GS15/2) - $3,836.49
   - Personnel Salary – 2% of $58,511 (GS9/5) – 1170.00

2. Physical Security – FY2012 - **$ 46,483.25**

   - Personnel salary – 10% of $155,500 (GS15/10) - $15,500.00
   - Personnel salary – 10% of $97,936.00 (GS13/4) - $9793.60
   - Visitor control for personnel and activities, based on 5% of guard costs (59,793.00) – 2,989.65
   - Access control system maintenance & monitoring & badging - $ 18,150.00

3. Classification Management – FY2012 - **$ 20,590.25**

   - Personnel salary estimate is based on 10% of $97,936.00 (GS13/4) – 9793.60
   - Personnel salary estimate based on 5% of $52,061.00 (GS7/8) - $2603.05
   - Personnel salary estimate based on 5% of $103,872.00 (GS13/6) - $5193.60
   - WNRC Costs - $3,000.00

4. Declassification – FY2012 - **$1,038.70**

   - Personnel salary estimate based on 5% of $103,872.00 (GS13/6) - $1038.70

5. Protection and Maintenance of Classified Information Systems - – FY2012 - **$979.36**
   No classified network – only standalone equipment
   - Personnel Salary estimate based on 1% of 97,936.00 (GS13/4) – $979.36

6. Operations Security and Technical Surveillance Countermeasures – FY2012 – N/A

7. Professional Education, Training, and awareness – FY2012 - **$2,500.00**
   - Comsec training expenses

8. Security Management, Oversight, and Planning - FY2012- **$ 60,749.70**
   - Personnel salary estimate based on 10% of $155,500 (GS15/10) - $15,500.00
   - Personnel salary estimate based on 20% of $97,936.00 (GS13/4) -$19,587.20
   - Personnel salary estimate based on 10% of $144,385.00 (GS15/6) - $14,438.50
   - Personnel salary estimate based on 10% of 112,224.00 - $11,224.00

9. Unique items - $0

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: Overseas Private Investment Corporation	**Fiscal Year:** 2013

Point of Contact:
(Name and phone number) (b) (6) [redacted]

Reporting Categories	Please use actual dollar figures.
1. Personnel Security *(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)*	$140,345.83
2. Physical Security *(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)*	$72,064.35
3. Classification Management *(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)*	$25,165.38
4. Declassification *(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)*	$0.00
5. Protection and Maintenance for Classified Information Systems *(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)*	$42,326.80
6. Operations Security and Technical Surveillance Countermeasures *(include personnel and operating expenses associated with OPSEC and TSCM)*	$0.00
7. Professional Education, Training, and Awareness *(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)*	$22,245.40
8. Security Management, Oversight, and Planning *(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))*	$55,798.90
9. Unique Items *(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)*	$0.00
TOTAL *(sum of items 1-9)*	$357,946.66

Narrative: *Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.*

5. OPIC used a contractor employee to mitigate a small spillage of classified onto the OPIC network, which constituted an unanticipated cost. Secondly, (b) (5) [redacted]
(b) (5)

7. OPIC developed a new computer-based Annual Refresher Training for personnel with access.

Instructions for Completing Form

I. General: The data reported will be Government cost estimates only. The estimates of resource costs should be reported, in the aggregate, for the following categories: (1) Personnel Security; (2) Physical Security; (3) Classification Management; (4) Declassification; (5) Protection and Maintenance for Classified information Systems; (6) Operations Security and Technical Surveillance Countermeasures; (7) Professional Education, Training, and Awareness; (8) Security Management, Oversight, and Planning; and (9) Unique Items. In reporting cost estimates associated with the security and management of classified information, please exclude all costs related to broad areas of assets protection (i.e., protection of property and personnel not specifically related to classified information). Counterintelligence* resources should also not be included in this data collection. If 51% or more of a resource is devoted to a classification-related activity, it should be included in this estimate. For those resources used for classification-related activities on a part-time basis, the total time devoted to these activities over a year must be at least 51% in order to be included in this estimate. Even though we no longer ask for the number of FTEs, the cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category.

II. Definitions of data to be reported: The primary categories are defined below along with related functional areas to be considered for inclusion. **Report only those cost estimates associated with classification-related activities** (programs that affect the security of classified information).

1. **Personnel Security:** A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

   Clearance Program: Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

   Initial Investigations: Completing and reviewing Personnel Security Questionnaire, initial screening, filing data in Central Personnel Database, forwarding to appropriate investigative authority, and the investigation itself.

   National Agency Check: Include only when used for basis for granting a clearance.

   Adjudication: Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

   Reinvestigations: Periodic recurring investigations of Government and contractor personnel.

   Polygraph: Substantive examinations in security screening process.

2. **Physical Security:** That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

   Physical Security Equipment: Any item, device, or system that is used primarily for the protection of classified information and installations.

   Protective Forces: All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

   Intrusion Detection and Assessment: Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

   Barrier/Controls: Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

---

* Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs. (48 CFR 970.0404-1)

Instructions for completing form, continued

Vital Components and Tamper-Safe Monitoring: Personnel and operating activities associated with the monitoring of tamper indicating devices for containers, doors, fences, etc., which reveal violations of containment integrity and posting and monitoring of anti-tamper warnings or signs.

Access Control/Badging: Personnel and hardware such as badging systems, card readers, turnstiles, metal detectors, cipher locks, CCTV, and other access control mechanisms to ensure that only authorized persons are allowed to enter or leave a classified facility.

Visitor Control: Personnel and activities associated with processing visitors for access to facilities holding classified information.

3. **Classification Management:** The system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, classified information, the protection of which is authorized by Executive Order or Statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information.

4. **Declassification:** The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive Order or Statute.

5. **Protection and Maintenance for Classified Information Systems:** A classified information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of classified information. Security of these systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats. This includes **TEMPEST** (short name referring to investigation, study, and control of compromising emanations from information systems equipment) and **Communications Security (COMSEC)** (measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material).

6. **Operations Security (OPSEC) and Technical Surveillance Countermeasures (TSCM):**

Operations Security (OPSEC): Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Technical Surveillance Countermeasures (TSCM): Personnel and operating expenses associated with the development, training, and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches, and telephone system searches.

7. **Professional Education, Training, and Awareness:** The establishment, maintenance, direction, support, and assessment of an information security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

8. **Security Management, Oversight, and Planning:** Development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities, and respond to management requests related to classified information.

Research, Test, and Evaluation: The development, management, and oversight of an acceptance and validation testing and evaluation program, corrective action reports and related documentation that addresses safeguards and security elements. The examination and testing of physical security systems (construction, facilities, and equipment) to ensure their effectiveness and operability and compliance with applicable directives.

Instructions for completing form, continued

Surveys, Reviews, Accreditation, and Assessments: Personnel and activities associated with surveys, reviews, accreditations, and assessments to determine the status of the security program and to evaluate its effectiveness; development and management of a facility survey and approval program; facility pre-survey; and information technology system accreditation.

Special Access Programs (SAP): Programs established for a specific class of classified information that impose safeguarding and access requirements that exceed those normally required for information at the same classification level. Unless specifically authorized by the President, only the Secretaries of State, Defense, Energy, and the Director of National Intelligence may create an SAP. Sensitive Compartmented Information (SCI) programs are not included as SAPs for the purpose of these estimates; rather SCI security costs are integrated and estimated throughout all categories as appropriate. Do not include costs here that have been reported under the other primary categories.

Security and Investigative Matters: The investigation of security incidents, infractions, and violations.

Industrial Security (Non-Contractor Costs): Those measures and resources directly identifiable as Government activities performed for the protection of classified information to which contractors, subcontractors, vendors, or suppliers have access or possession. Examples of such activities are industrial security reviews, surveys, and the granting of facility clearances, and National Industrial Security Program management and administration.

Foreign Ownership, Control, or Influence (FOCI): The development and management of a foreign ownership, control, or influence program; evaluation of FOCI submissions; the administration and monitoring of FOCI information and development of FOCI notifications.

9. **Unique Items:** Those department/agency-specific activities that are not reported in any of the primary categories but are nonetheless significant, and need to be included, should be noted in this category. Any unique item must include a narrative on why it should be included and how the figures were developed.

III. How to complete the security costs estimates form. The form (page 1) should include estimates of resource costs in the aggregate for each of the nine categories. The cost estimates reported should **not** include costs associated with the broader area of assets protection.

1. **Name of Department/Agency:** Self-explanatory.

2. **Reporting Categories:** List cost estimates in dollar amounts. The cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category. If there are no cost estimates to be reported for a particular category, indicate with a "0" in the appropriate block.

3. **Totals:** The totals for blocks 1-9 will automatically be placed in the appropriate block.

4. **Narrative:** In the narrative portion of the form, or in a separate attachment, provide a brief explanation of how cost estimates were determined. If there is a significant difference between the total figures for each fiscal year, explain the differences. Any figure reported within the Unique Items category should be clearly explained in the narrative portion.

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: Overseas Private Investment Corporation | **Fiscal Year:** 2014

Point of Contact:
(Name and phone number) (b) (6)

Reporting Categories

Please use actual dollar figures.

1. Personnel Security *(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)*	$172,661.00
2. Physical Security *(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)*	$90,559.00
3. Classification Management *(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)*	$31,783.00
4. Declassification *(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)*	$0.00
5. Protection and Maintenance for Classified Information Systems *(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)*	$23,022.00
6. Operations Security and Technical Surveillance Countermeasures *(include personnel and operating expenses associated with OPSEC and TSCM)*	$0.00
7. Professional Education, Training, and Awareness *(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)*	$14,198.00
8. Security Management, Oversight, and Planning *(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))*	$65,643.00
9. Unique Items *(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)*	$0.00
TOTAL *(sum of items 1-9)*	$397,866.00

Narrative: *Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.*

The increase of our total by $40,000 between the FY2013 report and FY2014 report relate to the hiring of one new FTE (who was reported as a partial year detailee in FY2013) and the promotion of another FTE from a GS 13 to a GS 14.

Instructions for Completing Form

I. General: The data reported will be Government cost estimates only. The estimates of resource costs should be reported, in the aggregate, for the following categories: (1) Personnel Security; (2) Physical Security; (3) Classification Management; (4) Declassification; (5) Protection and Maintenance for Classified information Systems; (6) Operations Security and Technical Surveillance Countermeasures; (7) Professional Education, Training, and Awareness; (8) Security Management, Oversight, and Planning; and (9) Unique Items. In reporting cost estimates associated with the security and management of classified information, please exclude all costs related to broad areas of assets protection (i.e., protection of property and personnel not specifically related to classified information). Counterintelligence* resources should also not be included in this data collection. If 51% or more of a resource is devoted to a classification-related activity, it should be included in this estimate. For those resources used for classification-related activities on a part-time basis, the total time devoted to these activities over a year must be at least 51% in order to be included in this estimate. Even though we no longer ask for the number of FTEs, the cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category.

II. Definitions of data to be reported: The primary categories are defined below along with related functional areas to be considered for inclusion. **Report only those cost estimates associated with classification-related activities** (programs that affect the security of classified information).

1. **Personnel Security:** A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

Clearance Program: Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

Initial Investigations: Completing and reviewing Personnel Security Questionnaire, initial screening, filing data in Central Personnel Database, forwarding to appropriate investigative authority, and the investigation itself.

National Agency Check: Include only when used for basis for granting a clearance.

Adjudication: Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

Reinvestigations: Periodic recurring investigations of Government and contractor personnel.

Polygraph: Substantive examinations in security screening process.

2. **Physical Security:** That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

Physical Security Equipment: Any item, device, or system that is used primarily for the protection of classified information and installations.

Protective Forces: All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

Intrusion Detection and Assessment: Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

Barrier/Controls: Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

---

* Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs. (48 CFR 970.0404-1)

Instructions for completing form, continued

Vital Components and Tamper-Safe Monitoring: Personnel and operating activities associated with the monitoring of tamper indicating devices for containers, doors, fences, etc., which reveal violations of containment integrity and posting and monitoring of anti-tamper warnings or signs.

Access Control/Badging: Personnel and hardware such as badging systems, card readers, turnstiles, metal detectors, cipher locks, CCTV, and other access control mechanisms to ensure that only authorized persons are allowed to enter or leave a classified facility.

Visitor Control: Personnel and activities associated with processing visitors for access to facilities holding classified information.

3. **Classification Management:** The system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, classified information, the protection of which is authorized by Executive Order or Statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information.

4. **Declassification:** The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive Order or Statute.

5. **Protection and Maintenance for Classified Information Systems:** A classified information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of classified information. Security of these systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats. This includes **TEMPEST** (short name referring to investigation, study, and control of compromising emanations from information systems equipment) and **Communications Security (COMSEC)** (measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material).

6. **Operations Security (OPSEC) and Technical Surveillance Countermeasures (TSCM):**

Operations Security (OPSEC): Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Technical Surveillance Countermeasures (TSCM): Personnel and operating expenses associated with the development, training, and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches, and telephone system searches.

7. **Professional Education, Training, and Awareness:** The establishment, maintenance, direction, support, and assessment of an information security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

8. **Security Management, Oversight, and Planning:** Development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities, and respond to management requests related to classified information.

Research, Test, and Evaluation: The development, management, and oversight of an acceptance and validation testing and evaluation program, corrective action reports and related documentation that addresses safeguards and security elements. The examination and testing of physical security systems (construction, facilities, and equipment) to ensure their effectiveness and operability and compliance with applicable directives.

Instructions for completing form, continued

Surveys, Reviews, Accreditation, and Assessments: Personnel and activities associated with surveys, reviews, accreditations, and assessments to determine the status of the security program and to evaluate its effectiveness; development and management of a facility survey and approval program; facility pre-survey; and information technology system accreditation.

Special Access Programs (SAP): Programs established for a specific class of classified information that impose safeguarding and access requirements that exceed those normally required for information at the same classification level. Unless specifically authorized by the President, only the Secretaries of State, Defense, Energy, and the Director of National Intelligence may create an SAP. Sensitive Compartmented Information (SCI) programs are not included as SAPs for the purpose of these estimates; rather SCI security costs are integrated and estimated throughout all categories as appropriate. Do not include costs here that have been reported under the other primary categories.

Security and Investigative Matters: The investigation of security incidents, infractions, and violations.

Industrial Security (Non-Contractor Costs): Those measures and resources directly identifiable as Government activities performed for the protection of classified information to which contractors, subcontractors, vendors, or suppliers have access or possession. Examples of such activities are industrial security reviews, surveys, and the granting of facility clearances, and National Industrial Security Program management and administration.

Foreign Ownership, Control, or Influence (FOCI): The development and management of a foreign ownership, control, or influence program; evaluation of FOCI submissions; the administration and monitoring of FOCI information and development of FOCI notifications.

9. **Unique Items:** Those department/agency-specific activities that are not reported in any of the primary categories but are nonetheless significant, and need to be included, should be noted in this category. Any unique item must include a narrative on why it should be included and how the figures were developed.

III. How to complete the security costs estimates form. The form (page 1) should include estimates of resource costs in the aggregate for each of the nine categories. The cost estimates reported should **not** include costs associated with the broader area of assets protection.

1. **Name of Department/Agency:** Self-explanatory.

2. **Reporting Categories:** List cost estimates in dollar amounts. The cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category. If there are no cost estimates to be reported for a particular category, indicate with a "0" in the appropriate block.

3. **Totals:** The totals for blocks 1-9 will automatically be placed in the appropriate block.

4. **Narrative:** In the narrative portion of the form, or in a separate attachment, provide a brief explanation of how cost estimates were determined. If there is a significant difference between the total figures for each fiscal year, explain the differences. Any figure reported within the Unique Items category should be clearly explained in the narrative portion.

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: Overseas Private Investment Corporation | **Fiscal Year:** 2015

Point of Contact:
(Name and phone number) (b) (6)

Please use actual dollar figures.

Reporting Categories

1. Personnel Security — $223,429.18
(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)

2. Physical Security — $94,785.39
(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)

3. Classification Management — $33,661.61
(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)

4. Declassification — $0.00
(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)

5. Protection and Maintenance for Classified Information Systems — $21,089.25
(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)

6. Operations Security and Technical Surveillance Countermeasures — $0.00
(include personnel and operating expenses associated with OPSEC and TSCM)

7. Professional Education, Training, and Awareness — $15,419.76
(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)

8. Security Management, Oversight, and Planning — $58,368.27
(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))

9. Unique Items — $0.00
(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)

TOTAL — $446,753.46
(sum of items 1-9)

Narrative: *Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.*

Increase in numbers is due to an additional FTE and a contractor.

Instructions for Completing Form

I. General: The data reported will be Government cost estimates only. The estimates of resource costs should be reported, in the aggregate, for the following categories: (1) Personnel Security; (2) Physical Security; (3) Classification Management; (4) Declassification; (5) Protection and Maintenance for Classified information Systems; (6) Operations Security and Technical Surveillance Countermeasures; (7) Professional Education, Training, and Awareness; (8) Security Management, Oversight, and Planning; and (9) Unique Items. In reporting cost estimates associated with the security and management of classified information, please exclude all costs related to broad areas of assets protection (i.e., protection of property and personnel not specifically related to classified information). Counterintelligence* resources should also not be included in this data collection. If 51% or more of a resource is devoted to a classification-related activity, it should be included in this estimate. For those resources used for classification-related activities on a part-time basis, the total time devoted to these activities over a year must be at least 51% in order to be included in this estimate. Even though we no longer ask for the number of FTEs, the cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category.

II. Definitions of data to be reported: The primary categories are defined below along with related functional areas to be considered for inclusion. **Report only those cost estimates associated with classification-related activities** (programs that affect the security of classified information).

1. **Personnel Security:** A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

   Clearance Program: Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

   Initial Investigations: Completing and reviewing Personnel Security Questionnaire, initial screening, filing data in Central Personnel Database, forwarding to appropriate investigative authority, and the investigation itself.

   National Agency Check: Include only when used for basis for granting a clearance.

   Adjudication: Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

   Reinvestigations: Periodic recurring investigations of Government and contractor personnel.

   Polygraph: Substantive examinations in security screening process.

2. **Physical Security:** That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

   Physical Security Equipment: Any item, device, or system that is used primarily for the protection of classified information and installations.

   Protective Forces: All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

   Intrusion Detection and Assessment: Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

   Barrier/Controls: Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

---

* Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs. (48 CFR 970.0404-1)

Instructions for completing form, continued

Vital Components and Tamper-Safe Monitoring: Personnel and operating activities associated with the monitoring of tamper indicating devices for containers, doors, fences, etc., which reveal violations of containment integrity and posting and monitoring of anti-tamper warnings or signs.

Access Control/Badging: Personnel and hardware such as badging systems, card readers, turnstiles, metal detectors, cipher locks, CCTV, and other access control mechanisms to ensure that only authorized persons are allowed to enter or leave a classified facility.

Visitor Control: Personnel and activities associated with processing visitors for access to facilities holding classified information.

3. **Classification Management:** The system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, classified information, the protection of which is authorized by Executive Order or Statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information.

4. **Declassification:** The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive Order or Statute.

5. **Protection and Maintenance for Classified Information Systems:** A classified information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of classified information. Security of these systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats. This includes **TEMPEST** (short name referring to investigation, study, and control of compromising emanations from information systems equipment) and **Communications Security (COMSEC)** (measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material).

6. **Operations Security (OPSEC) and Technical Surveillance Countermeasures (TSCM):**

Operations Security (OPSEC): Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Technical Surveillance Countermeasures (TSCM): Personnel and operating expenses associated with the development, training, and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches, and telephone system searches.

7. **Professional Education, Training, and Awareness:** The establishment, maintenance, direction, support, and assessment of an information security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

8. **Security Management, Oversight, and Planning:** Development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities, and respond to management requests related to classified information.

Research, Test, and Evaluation: The development, management, and oversight of an acceptance and validation testing and evaluation program, corrective action reports and related documentation that addresses safeguards and security elements. The examination and testing of physical security systems (construction, facilities, and equipment) to ensure their effectiveness and operability and compliance with applicable directives.

Instructions for completing form, continued

Surveys, Reviews, Accreditation, and Assessments: Personnel and activities associated with surveys, reviews, accreditations, and assessments to determine the status of the security program and to evaluate its effectiveness; development and management of a facility survey and approval program; facility pre-survey; and information technology system accreditation.

Special Access Programs (SAP): Programs established for a specific class of classified information that impose safeguarding and access requirements that exceed those normally required for information at the same classification level. Unless specifically authorized by the President, only the Secretaries of State, Defense, Energy, and the Director of National Intelligence may create an SAP. Sensitive Compartmented Information (SCI) programs are not included as SAPs for the purpose of these estimates; rather SCI security costs are integrated and estimated throughout all categories as appropriate. Do not include costs here that have been reported under the other primary categories.

Security and Investigative Matters: The investigation of security incidents, infractions, and violations.

Industrial Security (Non-Contractor Costs): Those measures and resources directly identifiable as Government activities performed for the protection of classified information to which contractors, subcontractors, vendors, or suppliers have access or possession. Examples of such activities are industrial security reviews, surveys, and the granting of facility clearances, and National Industrial Security Program management and administration.

Foreign Ownership, Control, or Influence (FOCI): The development and management of a foreign ownership, control, or influence program; evaluation of FOCI submissions; the administration and monitoring of FOCI information and development of FOCI notifications.

9. **Unique Items:** Those department/agency-specific activities that are not reported in any of the primary categories but are nonetheless significant, and need to be included, should be noted in this category. Any unique item must include a narrative on why it should be included and how the figures were developed.

III. How to complete the security costs estimates form. The form (page 1) should include estimates of resource costs in the aggregate for each of the nine categories. The cost estimates reported should **not** include costs associated with the broader area of assets protection.

1. **Name of Department/Agency:** Self-explanatory.

2. **Reporting Categories:** List cost estimates in dollar amounts. The cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category. If there are no cost estimates to be reported for a particular category, indicate with a "0" in the appropriate block.

3. **Totals:** The totals for blocks 1-9 will automatically be placed in the appropriate block.

4. **Narrative:** In the narrative portion of the form, or in a separate attachment, provide a brief explanation of how cost estimates were determined. If there is a significant difference between the total figures for each fiscal year, explain the differences. Any figure reported within the Unique Items category should be clearly explained in the narrative portion.

AGENCY SECURITY CLASSIFICATION COSTS ESTIMATES

Department/Agency: Overseas Private Investment Corporation | **Fiscal Year:** 2016

Point of Contact:
(Name and phone number) (b) (6)

Reporting Categories

Please use actual dollar figures.

1. Personnel Security *(include clearance program, initial investigations, national agency checks when used as basis for granting a clearance, adjudication, reinvestigation, polygraph associated with classification-related activities)*	$291,847.30
2. Physical Security *(include physical security equipment, protective forces, intrusion detection and assessment, barrier/controls, tamper-safe monitoring, access control/badging, visitor control associated with classification-related activities)*	$137,751.95
3. Classification Management *(include resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information)*	$28,828.68
4. Declassification *(include resources used to identify and process information subject to the automatic, systematic, discretionary, or mandatory review programs authorized by Executive Order or Statute)*	$0.00
5. Protection and Maintenance for Classified Information Systems *(include resources used to protect and maintain classified information systems from unauthorized access or modification of information, and against the denial of service to authorized users, including measures necessary to detect, document, and counter such threats)*	$11,805.40
6. Operations Security and Technical Surveillance Countermeasures *(include personnel and operating expenses associated with OPSEC and TSCM)*	$0.00
7. Professional Education, Training, and Awareness *(include resources used to establish, maintain, direct, support, and assess an information security training and awareness program; certification and approval of the training program; development, management, and maintenance of training records; training of personnel to perform tasks; and qualification and/or certification of personnel associated with classification-related activities)*	$11,886.25
8. Security Management, Oversight, and Planning *(include resources associated with research, test, and evaluation; surveys, reviews, accreditation, and assessments; special access programs; security and investigative matters; industrial security; and foreign ownership, control, or influence (FOCI))*	$142,184.13
9. Unique Items *(include department/agency-specific activities not reported in any of the categories listed above, but are nonetheless significant and need to be included)*	$0.00
TOTAL *(sum of items 1-9)*	$624,303.71

Narrative: *Provide a brief explanation of any significant difference between last year's and this year's cost estimates. Explain items entered into block 9, Unique Items.*

Instructions for Completing Form

I. General: The data reported will be Government cost estimates only. The estimates of resource costs should be reported, in the aggregate, for the following categories: (1) Personnel Security; (2) Physical Security; (3) Classification Management; (4) Declassification; (5) Protection and Maintenance for Classified information Systems; (6) Operations Security and Technical Surveillance Countermeasures; (7) Professional Education, Training, and Awareness; (8) Security Management, Oversight, and Planning; and (9) Unique Items. In reporting cost estimates associated with the security and management of classified information, please exclude all costs related to broad areas of assets protection (i.e., protection of property and personnel not specifically related to classified information). Counterintelligence* resources should also not be included in this data collection. If 51% or more of a resource is devoted to a classification-related activity, it should be included in this estimate. For those resources used for classification-related activities on a part-time basis, the total time devoted to these activities over a year must be at least 51% in order to be included in this estimate. Even though we no longer ask for the number of FTEs, the cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category.

II. Definitions of data to be reported: The primary categories are defined below along with related functional areas to be considered for inclusion. **Report only those cost estimates associated with classification-related activities** (programs that affect the security of classified information).

1. **Personnel Security:** A series of interlocking and mutually supporting program elements that initially establish a Government or contractor employee's eligibility, and ensure suitability for the continued access to classified information.

Clearance Program: Personnel and activities to determine eligibility and suitability for initial or continuing access to classified information or activities.

Initial Investigations: Completing and reviewing Personnel Security Questionnaire, initial screening, filing data in Central Personnel Database, forwarding to appropriate investigative authority, and the investigation itself.

National Agency Check: Include only when used for basis for granting a clearance.

Adjudication: Screening and analysis of personnel security cases for determining eligibility for classified access authorizations and appeals process.

Reinvestigations: Periodic recurring investigations of Government and contractor personnel.

Polygraph: Substantive examinations in security screening process.

2. **Physical Security:** That portion of security concerned with physical measures designed to safeguard and protect classified facilities and information, domestic or foreign.

Physical Security Equipment: Any item, device, or system that is used primarily for the protection of classified information and installations.

Protective Forces: All personnel and operating costs associated with protective forces used to safeguard classified information or installations, to include but not limited to salaries, overtime, benefits, materials and supplies, equipment and facilities, vehicles, aircraft, training, communications equipment, and management.

Intrusion Detection and Assessment: Alarms, sensors, protective lighting, and their control systems; and the assessment of the reliability, accuracy, timeliness, and effectiveness of those systems used to safeguard classified information or installations.

Barrier/Controls: Walls, fences, barricades, or other fabricated or natural impediments to restrict, limit, delay, or deny entry into a classified installation.

---

* Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or international terrorist activities, but not including personnel, physical, document, or communications security programs. (48 CFR 970.0404-1)

Instructions for completing form, continued

Vital Components and Tamper-Safe Monitoring: Personnel and operating activities associated with the monitoring of tamper indicating devices for containers, doors, fences, etc., which reveal violations of containment integrity and posting and monitoring of anti-tamper warnings or signs.

Access Control/Badging: Personnel and hardware such as badging systems, card readers, turnstiles, metal detectors, cipher locks, CCTV, and other access control mechanisms to ensure that only authorized persons are allowed to enter or leave a classified facility.

Visitor Control: Personnel and activities associated with processing visitors for access to facilities holding classified information.

3. **Classification Management:** The system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, classified information, the protection of which is authorized by Executive Order or Statute. Classification management encompasses those resources used to identify, control, transfer, transmit, retrieve, inventory, archive, declassify, or destroy classified information.

4. **Declassification:** The authorized change in the status of information from classified information to unclassified information. It encompasses those resources used to identify and process information subject to the automatic, systematic, or mandatory review programs authorized by Executive Order or Statute.

5. **Protection and Maintenance for Classified Information Systems:** A classified information system is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of classified information. Security of these systems involves the protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document and counter such threats. This includes **TEMPEST** (short name referring to investigation, study, and control of compromising emanations from information systems equipment) and **Communications Security (COMSEC)** (measures and controls taken to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of COMSEC material).

6. **Operations Security (OPSEC) and Technical Surveillance Countermeasures (TSCM):**

Operations Security (OPSEC): Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.

Technical Surveillance Countermeasures (TSCM): Personnel and operating expenses associated with the development, training, and application of technical security countermeasures such as non-destructive and destructive searches, electromagnetic energy searches, and telephone system searches.

7. **Professional Education, Training, and Awareness:** The establishment, maintenance, direction, support, and assessment of an information security training and awareness program; the certification and approval of the training program; the development, management, and maintenance of training records; the training of personnel to perform tasks associated with their duties; and qualification and/or certification of personnel before assignment of security responsibilities related to classified information.

8. **Security Management, Oversight, and Planning:** Development and implementation of plans, procedures, and actions to accomplish policy requirements, develop budget and resource requirements, oversee organizational activities, and respond to management requests related to classified information.

Research, Test, and Evaluation: The development, management, and oversight of an acceptance and validation testing and evaluation program, corrective action reports and related documentation that addresses safeguards and security elements. The examination and testing of physical security systems (construction, facilities, and equipment) to ensure their effectiveness and operability and compliance with applicable directives.

Instructions for completing form, continued

Surveys, Reviews, Accreditation, and Assessments: Personnel and activities associated with surveys, reviews, accreditations, and assessments to determine the status of the security program and to evaluate its effectiveness; development and management of a facility survey and approval program; facility pre-survey; and information technology system accreditation.

Special Access Programs (SAP): Programs established for a specific class of classified information that impose safeguarding and access requirements that exceed those normally required for information at the same classification level. Unless specifically authorized by the President, only the Secretaries of State, Defense, Energy, and the Director of National Intelligence may create an SAP. Sensitive Compartmented Information (SCI) programs are not included as SAPs for the purpose of these estimates; rather SCI security costs are integrated and estimated throughout all categories as appropriate. Do not include costs here that have been reported under the other primary categories.

Security and Investigative Matters: The investigation of security incidents, infractions, and violations.

Industrial Security (Non-Contractor Costs): Those measures and resources directly identifiable as Government activities performed for the protection of classified information to which contractors, subcontractors, vendors, or suppliers have access or possession. Examples of such activities are industrial security reviews, surveys, and the granting of facility clearances, and National Industrial Security Program management and administration.

Foreign Ownership, Control, or Influence (FOCI): The development and management of a foreign ownership, control, or influence program; evaluation of FOCI submissions; the administration and monitoring of FOCI information and development of FOCI notifications.

9. **Unique Items:** Those department/agency-specific activities that are not reported in any of the primary categories but are nonetheless significant, and need to be included, should be noted in this category. Any unique item must include a narrative on why it should be included and how the figures were developed.

III. How to complete the security costs estimates form. The form (page 1) should include estimates of resource costs in the aggregate for each of the nine categories. The cost estimates reported should **not** include costs associated with the broader area of assets protection.

1. **Name of Department/Agency:** Self-explanatory.

2. **Reporting Categories:** List cost estimates in dollar amounts. The cost of personnel associated with the security of classified information should be included in the overall cost estimate for each category. If there are no cost estimates to be reported for a particular category, indicate with a "0" in the appropriate block.

3. **Totals:** The totals for blocks 1-9 will automatically be placed in the appropriate block.

4. **Narrative:** In the narrative portion of the form, or in a separate attachment, provide a brief explanation of how cost estimates were determined. If there is a significant difference between the total figures for each fiscal year, explain the differences. Any figure reported within the Unique Items category should be clearly explained in the narrative portion.